(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105635147 A
(43)申请公布日 2016.06.01

(21)申请号 201511020141.0

(22)申请日 2015.12.30

(71)申请人 深圳市图雅丽特种技术有限公司
地址 518000 广东省深圳市龙华新区大浪办事处浪口社区华昌路华富工业园第8栋厂房一层

(72)发明人 龙刚 蒋灿 韦沛余

(74)专利代理机构 深圳市硕法知识产权代理事务所（普通合伙） 44321
代理人 李姝

(51)Int.Cl.
H04L 29/06(2006.01)

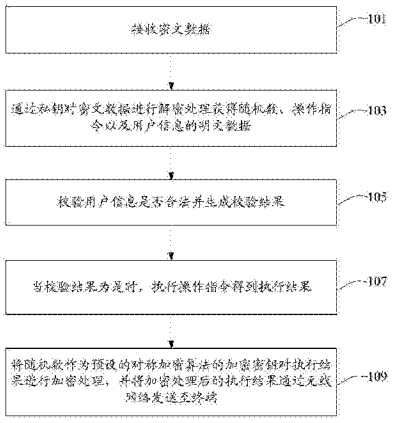
权利要求书2页 说明书8页 附图5页

(54)发明名称

基于车载特种装备系统的数据安全传输方法及系统

(57)摘要

本发明涉及一种基于车载特种装备系统的数据加密传输方法和系统，其中该方法包括：接收密文数据，密文数据是终端通过公钥对包含随机数、操作指令以及用户信息的字符串进行加密处理后发送至车辆的；通过私钥对密文数据进行解密处理获得随机数、操作指令以及用户信息的明文数据；校验用户信息是否合法并生成校验结果；当校验结果为是时，执行操作指令得到执行结果；将随机数作为预设的对称加密算法的加密密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端，使得终端将随机数作为对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。上述方法和系统提高了终端与车辆之间数据传输的安全性。



CN 105635147 A

1.一种基于车载特种装备系统的数据加密传输方法，应用于车辆，其特征在于，所述方法包括：

接收密文数据，所述密文数据是终端通过公钥对包含随机数、操作指令以及用户信息的字符串进行加密处理后发送至车辆的；

通过私钥对所述密文数据进行解密处理获得所述随机数、所述操作指令以及用户信息的明文数据；

校验所述用户信息是否合法并生成校验结果；

当校验结果为是时，执行所述操作指令得到执行结果；

将随机数作为预设的对称加密算法的加密密钥对所述执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端，使得所述终端将随机数作为所述对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。

2.根据权利要求1所述的方法，其特征在于，当校验结果为否时，所述方法还包括：

生成执行操作指令失败的反馈信息；

将所述随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端。

3.根据权利要求1所述的方法，其特征在于，所述方法还包括：

生成密钥对，所述密钥对包括私钥和公钥；

将私钥存储至安全区域，并将所述公钥和预设的车辆标识上传至服务器，所述服务器为所述终端提供公钥和车辆标识的下载服务。

4.根据权利要求3所述的方法，其特征在于，所述生成密钥对的步骤，包括：

生成多个质数，并从多个质数中随机选择不相等的两个质数；

将所述两个质数作为密钥因子，通过预设的非对称加密算法生成包含公钥和私钥的密钥对。

5.一种基于车载特种装备系统的数据加密传输方法，应用于终端，其特征在于，所述方法包括：

获取公钥以及车辆标识；

接收用户对所述车辆标识对应的车辆触发的操作指令；

生成随机数，并通过所述公钥对包含所述随机数、所述操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据；

通过无线网络将所述密文数据发送至车辆，使得所述车辆通过私钥对密文数据进行解密处理得到明文数据，并校验用户信息是否合法，当校验结果为是时，执行所述操作指令得到执行结果；

接收车辆发送的执行结果，所述执行结果是车辆将随机数作为加密密钥对执行结果进行加密处理得到的；

将随机数作为所述对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。

6.根据权利要求5所述的方法，其特征在于，所述方法还包括：

接收车辆发送的生成执行操作指令失败的反馈信息，所述车辆将随机数作为预设的对称加密算法的加密密钥对所述反馈信息进行了加密处理；

将所述随机数作为对称加密算法的解密密钥对所述反馈信息进行解密处理，获得明文的反馈信息。

7.一种基于车载特种装备系统的数据加密传输系统，其特征在于，包括车辆和终端；其中，所述终端用于从服务器下载公钥和车辆标识；接收用户对所述车辆标识对应的车辆触发的操作指令；生成随机数；通过所述公钥对包含所述随机数、所述操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据；通过无线网络将所述密文数据发送至车辆；接收车辆发送的执行结果；将随机数作为解密密钥对加密的执行结果进行解密，得到明文的执行结果；接收车辆发送的经过加密处理的反馈信息，将所述随机数作为预设的对称加密算法的解密密钥对所述反馈信息进行解密处理，获得明文的反馈信息。

所述车辆用于接收终端发送的密文数据；通过私钥对所述密文数据进行解密处理获得所述随机数、所述操作指令以及用户信息的明文数据；校验所述用户信息是否合法并生成校验结果；当校验结果为是时，执行所述操作指令得到执行结果；将随机数作为对称加密算法的密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端；当校验结果为否时，生成执行操作指令失败的反馈信息；将所述随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端。

8.一种车载特种装备系统，其特征在于，包括车载电脑、无线收发器、加解密器以及校验器；其特征在于，所述无线收发器与所述加解密器连接，所述加解密器与所述校验器连，所述车载电脑分别与所述加解密器以及所述校验器连接；

所述加解密器用于存储车辆标识，生成包含公钥和私钥的密钥对，存储所述私钥，对终端发送的密文数据通过私钥进行解密处理，获得明文的随机数、操作指令以及用户信息；将随机数作为对称加密算法的密钥对执行结果和反馈信息进行加密处理；

所述无线收发器用于接收终端发送的通过公钥对包含随机数、操作指令以及用户信息进行加密处理得到的密文数据，将加解密器对执行结果进行加密处理后的执行结果发送至终端；

所述校验器用于获取加解密器传输的用户信息；校验用户信息是否合法，生成校验结果并传输至车载特种装备系统；

所述车载电脑用于当校验结果为是时，执行操作指令，并将执行结果发送至加解密器中进行加密处理，当校验结果为否时，生成执行命令失败的反馈信息并发送至所述加解密器。

9.根据权利要求8所述的车辆，其特征在于，所述加解密器还用于将公钥以及车辆标识发送至无线收发器；所述无线收发器还用于将所述公钥和车辆标识上传至服务器，所述服务器为终端提供公钥和车辆标识的下载服务。

10.一种车辆，其特征在于，所述车辆安装有如权利要求8至9任意一项所述的特种装备车载系统。

基于车载特种装备系统的数据安全传输方法及系统

技术领域

[0001] 本发明涉及通讯网络安全技术领域，特别是涉及一种基于车载特种装备系统的数据安全传输方法及系统。

背景技术

[0002] 随着汽车互联网技术的不断发展，未来汽车的联网程度和内外数据交换的容量都将日益增多。先进的车载联网技术在给用户带来便捷体验的同时，也会越来越多的带来安全问题。例如，车辆以直接或者间接方式连接互联网容易暴露于恶意软件的代码和数据攻击之下，使车辆受控行驶，急踩刹车，未经允许自动开关车门，甚至会造成交通事故。因此连接到因特网的车载特种装备系统的安全传输尤为重要。

[0003] 目前基于车联网的汽车远程数据传输，因为未充分考虑安全问题，没有对数据进行安全加密而是以明文传输或者只是进行简单的加密后进行传输。随着超级计算机的普及传统简单加密技术，无法确保车载特种装备系统的数据在互联网上传输的安全性。

发明内容

[0004] 基于此，有必要针对上述技术问题，提供一种能提高数据传输安全性的基于车载特种装备系统的数据安全传输方法及系统。

[0005] 一种基于车载特种装备系统的数据加密传输方法，应用于车辆，所述方法包括：

[0006] 接收密文数据，所述密文数据是终端通过公钥对包含随机数、操作指令以及用户信息的字符串进行加密处理后发送至车辆的；

[0007] 通过私钥对所述密文数据进行解密处理获得所述随机数、所述操作指令以及用户信息的明文数据；

[0008] 校验所述用户信息是否合法并生成校验结果；

[0009] 当校验结果为是时，执行所述操作指令得到执行结果；

[0010] 将随机数作为预设的对称加密算法的加密密钥对所述执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端，使得所述终端将随机数作为所述对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。

[0011] 在其中一个实施例中，当校验结果为否时，所述方法还包括：

[0012] 生成执行操作指令失败的反馈信息；

[0013] 将所述随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端。

[0014] 在其中一个实施例中，所述方法还包括：

[0015] 生成密钥对，所述密钥对包括私钥和公钥；

[0016] 将私钥存储至安全区域，并将所述公钥和预设的车辆标识上传至服务器，所述服务器为所述终端提供公钥和车辆标识的下载服务。

[0017] 在其中一个实施例中，所述生成密钥对的步骤，包括：

[0018] 生成多个质数，并从多个质数中随机选择不相等的两个质数；

[0019] 将所述两个质数作为密钥因子，通过预设的非对称加密算法生成包含公钥和私钥的密钥对。

[0020] 一种基于车载特种装备系统的数据加密传输方法，应用于终端，所述方法包括：

[0021] 获取公钥以及车辆标识；

[0022] 接收用户对所述车辆标识对应的车辆触发的操作指令；

[0023] 生成随机数，并通过所述公钥对包含所述随机数、所述操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据；

[0024] 通过无线网络将所述密文数据发送至车辆，使得所述车辆通过私钥对密文数据进行解密处理得到明文数据，并校验用户信息是否合法，当校验结果为是时，执行所述操作指令得到执行结果；

[0025] 接收车辆发送的执行结果，所述执行结果是车辆将随机数作为加密密钥对执行结果进行加密处理得到的；

[0026] 将随机数作为所述对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。

[0027] 在其中一个实施例中，所述方法还包括：

[0028] 接收车辆发送的生成执行操作指令失败的反馈信息，所述车辆将随机数作为预设的对称加密算法的加密密钥对所述反馈信息进行了加密处理；

[0029] 将所述随机数作为对称加密算法的解密密钥对所述反馈信息进行解密处理，获得明文的反馈信息。

[0030] 一种基于车载特种装备系统的数据加密传输系统，包括车辆和终端；所述终端用于从服务器下载公钥和车辆标识；接收用户对所述车辆标识对应的车辆触发的操作指令；生成随机数；通过所述公钥对包含所述随机数、所述操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据；通过无线网络将所述密文数据发送至车辆；接收车辆发送的执行结果；将随机数作为解密密钥对加密的执行结果进行解密，得到明文的执行结果；接收车辆发送的经过加密处理的反馈信息，将所述随机数作为预设的对称加密算法的解密密钥对所述反馈信息进行解密处理，获得明文的反馈信息。

[0031] 所述车辆用于接收终端发送的密文数据；通过私钥对所述密文数据进行解密处理获得所述随机数、所述操作指令以及用户信息的明文数据；校验所述用户信息是否合法并生成校验结果；当校验结果为是时，执行所述操作指令得到执行结果；将随机数作为对称加密算法的密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端；当校验结果为否时，生成执行操作指令失败的反馈信息；将所述随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端。

[0032] 一种车载特种装备系统，包括车载电脑、无线收发器、加解密器以及校验器；所述无线收发器与所述加解密器连接，所述加解密器与所述校验器连，所述车载电脑分别与所述加解密器以及所述校验器连接；

[0033] 所述加解密器用于存储车辆标识，生成包含公钥和私钥的密钥对，存储所述私钥，对终端发送的密文数据通过私钥进行解密处理，获得明文的随机数、操作指令以及用户信

息;将随机数作为对称加密算法的密钥对执行结果和反馈信息进行加密处理;

[0034] 所述无线收发器用于接收终端发送的通过公钥对包含随机数、操作指令以及用户信息进行加密处理得到的密文数据,将加解密器对执行结果进行加密处理后的执行结果发送至终端;

[0035] 所述校验器用于获取加解密器传输的用户信息;校验用户信息是否合法,生成校验结果并传输至车载特种装备系统;

[0036] 所述车载电脑用于当校验结果为是时,执行操作指令,并将执行结果发送至加解密器中进行加密处理,当校验结果为否时,生成执行命令失败的反馈信息并发送至所述加解密器。

[0037] 在其中一个实施例中,所述加解密器还用于将公钥以及车辆标识发送至无线收发器;所述无线收发器还用于将所述公钥和车辆标识上传至服务器,所述服务器为终端提供公钥和车辆标识的下载服务。

[0038] 一种车辆,所述车辆安装有特种装备车载系统。

[0039] 上述基于车载特种装备系统的数据加密传输方法及系统,终端向车辆传输的数据采用了私钥和公钥的密钥对进行加解密,而车辆向终端传输的数据将随机数作为对称加密算法的加解密的密钥因子进行加解密,由于加密与解密采用了不同的密钥因而增加了密码的破解难度,提高了终端与车辆之间传输数据的安全性。

附图说明

[0040] 图1为一个实施例中基于车载特种装备系统的数据加密传输方法的流程示意图;

[0041] 图2为另一个实施例中基于车载特种装备系统的数据加密传输方法的流程示意图;

[0042] 图3为一个实施例中基于车载特种装备系统的数据加密传输方法的流程示意图;

[0043] 图4为一个实施例中基于车载特种装备系统的数据加密传输系统的应用场景图;

[0044] 图5为一个实施例中车载特种装备系统的结构示意图。

具体实施方式

[0045] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0046] 在一个实施例中,参考图1,一种基于车载特种装备系统的数据加密传输方法,应用于车辆,该方法包括如下步骤:

[0047] 步骤101,接收密文数据。

[0048] 本实施例中,密文数据是终端通过公钥对包含随机数、操作指令以及用户信息的字符串进行加密处理后发送至车辆的。终端包括但不限于遥控器、智能手机、平板电脑、笔记本电脑以及台式电脑等。

[0049] 步骤103,通过私钥对密文数据进行解密处理获得随机数、操作指令以及用户信息的明文数据。

[0050] 本实施例中,车辆的无线收发器接收到密文数据后,进一步的将密文数据传输至

加解密器中，由加解密器中存储的私钥对密文数据进行解密。私钥存储在加解密器的安全存储区域。例如，安全存储区域为SoC(System on a Chip)片内OTP(One Time Programable)区域。使用私钥对密文数据进行解密得到明文数据。具体的，私钥为RSA私钥。RSA私钥解密公式如下：cd＝n(mod N)其中的c为密文数据，(N,d)是RSA私钥，计算出n，则n为解密后的明文数据。加解密器，包括RSA加解密运算器。

[0051] 步骤105，校验用户信息是否合法并生成校验结果。

[0052] 本实施例中，用户信息用于作为车辆使用者的身份标识。具体的，用户信息包括但不限于用户身份ID或者终端ID。例如，终端为手机时，用户信息可以是手机号码或身份证号码。为了防止恶意用户操控车辆，在执行操作指令之前需要验证用户是否为合法用户。在一个实施例中，将用户信息预先固化到车辆的校验器中的安全存储区域，以等待后续校验使用。检验用户信息是否合法，是将校验器中已存储的用户信息与终端发送的用户信息进行比对，当两者完全相同时表示用户信息合法，否则用户信息非法。

[0053] 步骤107，当校验结果为是时，执行操作指令得到执行结果。

[0054] 本实施例中，当校验结果为是时，表示给车辆下达操作指令的用户是合法的，进一步的，通过车辆中的车载特种装备系统执行操作指令，并得到执行结果。例如，操作指令为车辆空调的关闭指令，则执行结果为空调是否成功关闭的信息。将执行结果以字符串的形式传输至加解密器中，由加解密器对其进行加密处理。

[0055] 步骤109，将随机数作为预设的对称加密算法的加密密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端。

[0056] 本实施例中，终端将随机数作为对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。通常车辆反馈至终端的数据不会影响到终端的安全，所以采用对称加密算法进行加解密，由于加密与解密的密钥都是同一个，因而加解密的速度快，将终端生成的随机数作为加解密的密钥，使得每次传输的数据的密钥都不相同，既在不影响数据的安全性的同时提高了数据的传输效率。优选的，对称加密算法为AES算法，加解密器，包括AES加解密运算器。

[0057] 上述基于车载特种装备系统的数据加密传输方法，终端向车辆传输的数据采用了私钥和公钥的密钥对进行加解密，而车辆向终端传输的数据将随机数作为对称加密算法的加解密的密钥因子进行加解密，由于加密与解密采用了不同的密钥因而增加了密码的破解难度，提高了终端与车辆之间传输数据的安全性。

[0058] 在一个实施例中，参考图2，基于车载特种装备系统的数据加密传输方法还包括：

[0059] 步骤106，当校验结果为否时，生成执行操作指令失败的反馈信息。

[0060] 步骤108，将随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端。

[0061] 本实施例中，校验结果为否表示车辆不会执行操作指令。出现这种情况可能是非法用户想要操控车辆，也可能是黑客对终端发送至车辆的数据进行了篡改，还可能是数据在加密或者传输过程中出现了数据丢失的情况。此时车辆的车载特种装备系统将不会执行操作指令，直接将终端发送的数据丢弃掉。

[0062] 在一个实施例中，车辆的车载特种装备系统还可以进一步的分析造成校验失败的原因，获取校验失败的原因对应的错误代码，将错误代码的字符串反馈至终端，使得终端的

用户可以清楚了解到执行操作指令失败的原因。

[0063] 在一个实施例中，基于车载特种装备系统的数据加密传输方法还包括：生成密钥对，密钥对包括私钥和公钥；将私钥存储至安全区域，并将公钥和预设的车辆标识上传至服务器。服务器为终端提供公钥和车辆标识的下载服务。公钥需要提供给终端，车辆可以通过无线网络直接发送至终端，还可以将公钥上传至服务器，由服务器为终端提供下载服务。

[0064] 本实施例中，密钥对中的私钥存储在车辆的安全区域，用于解密数据，公钥存储在终端用于对发送的数据进行加密。由于数据的加解密采用的是不相同的密钥，因而使得加密的数据不易破解。具体的，服务器上存储的公钥的格式为x.509格式。

[0065] 在一个实施例中，生成密钥对的步骤包括：生成多个质数，并从多个质数中随机选择不相等的两个质数；将两个质数作为密钥因子，通过预设的非对称加密算法生成包含公钥和私钥的密钥对。

[0066] 具体的，通过车辆的加解密器中的模密运算控制器和随机数发生器产生随机数，从随机数中选取两个随机数p和q，判断p和q是不是质数并且互质，若是则将p和q作为密钥对的密钥因子。若否则继续产生随机数p和随机数q，一直到满足条件为止。车辆的加解密器，一般采用基于SoC芯片的硬件控制加速器，如模密运算器、AES、RSA加密运算器等。

[0067] 在一个实施例中，非对称加密算法为RSA算法，由RSA算法生成密钥对包括以下步骤：车辆的加解密器随机生成质数，并从质数中选取两个大的质数p和q，且p不等于q，p和q作为密钥因子，计算N＝pq。进一步的，根据欧拉函数，求r＝(p-1)(q-1)；选择一个小于r的整数e，求得e关于模r的模反元素，命名为d。(模反元素存在，当且仅当e与r互质)；将p和q的记录销毁；(N,e)是公钥，(N,d)是私钥。为了使得密钥密文数据的速度不易太慢，同时加密后的数据不易破解，需要为密钥选择合适的字节长度。优选的，密钥对的字节长度为2048bit以上，e为3或者65537。

[0068] 如图3所示，在一个实施例中，提供的一种基于车载特种装备系统的数据加密传输方法，应用于终端，该方法包括如下步骤：

[0069] 步骤301，获取公钥以及车辆标识。

[0070] 本实施例中，车辆标识作为车辆的唯一身份的标示。具体的，车辆标识包括但不限于：车辆的发动机编号、车牌号码以及车辆WIFI的MAC地址等。车辆标识预先存储在车辆的加解密器中，车辆加解密器生成的非对称的密钥对中的公钥将保存在终端。车辆连入互联网后，将公钥以及车辆标识上传至服务器中。用户通过终端连入互联网，在获得服务器的授权后将公钥和车辆标识下载至本地。作为解密用的私钥对应确保数据的安全尤为重要，因此将私钥存储至加解密器中的安全存储区域。

[0071] 步骤302，接收用户对车辆标识对应的车辆触发的操作指令。

[0072] 本实施例中，终端中运行一与车辆进行数据交互的应用，用户在应用的登陆界面上输入登录信息(用户名和登陆密码)，在登录信息验证通过后便可在软件的操作界面上触发对车辆的操作指令。具体可以通过按钮或者触摸来触发操作指令。这里的操作指令并不特指操控车辆的指令，还包括获取车辆状态数据的指令。例如，车辆的里程数据或者油耗数据等。

[0073] 步骤303，生成随机数，并通过公钥对包含随机数、操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据。

[0074] 本实施例中，终端在将操作指令发送至车辆之前，为了确保数据传输的安全性需要对操作指令进行加密。利用公钥对随机数、操作指令以及用户信息组成的字符串做加密处理。具体的，通过RSA公钥进行加密，由于RSA属于非对称密钥算法，即加密和解密为不同的密钥，RSA公钥加密后，只能用唯一的私钥解密，而私钥存储在车辆安全存储区域内，可以确保私钥的安全性，因而加密后的数据不易被非法用户破解。

[0075] 步骤304，通过无线网络将密文数据发送至车辆。

[0076] 本实施例中，终端通过无线传输模块将密文数据发送至车辆。具体的，无线传输模块包括但不限于：GSM、GPRS、3G、4G以及WIFI等无线传输模块。车辆通过私钥对密文数据进行解密处理得到明文数据，并校验用户信息是否合法，当校验结果为是时，执行操作指令得到执行结果。

[0077] 步骤305，接收车辆发送的执行结果，执行结果是车辆将随机数作为加密密钥通过预设的对称加密算法对执行结果进行加密处理得到的。

[0078] 步骤306，将随机数作为对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果。

[0079] 本实施例中，由于车辆对执行结果的加密使用的加密密钥用的是终端发送的随机数，因而终端只需将随机数作为对称加密算法的解密密钥对加密后的执行结果进行解密，即可获得明文的执行结果。具体的，对称加加密算法为AES算法，由于AES为高级对称加解密算法，加密和解密使用相同的密钥，因此加解密的速度快。而采用随机数作为加解密密钥，使得每次的加解密的密钥都不相同，增加了破解难度使得数据传输也更安全。终端获得明文的执行结果后通过终端进行展示。

[0080] 终端发送到汽车的指令会影响行车安全，因而在发送数据之前先在终端通过公钥进行加密，通过车辆中的私钥对加密后的密文数据进行解密，而车辆返回至终端的数据对终端的安全性影响小，因此使用了对称的加密密钥进行加解密。非对称密钥对进行加解密运算花费的时间长但是安全性好，车辆返回至终端数据多，采用对称密钥进行加解密运算花费的时间短，一次一密钥安全性也能得到保证。既提高了终端与车辆之间数据交互的安全性，还确保了数据传输的效率。

[0081] 在一个实施例中，提供的一种基于车载特种装备系统的数据加密传输方法该方法应用于终端，还包括如下步骤：接收车辆发送的生成执行操作指令失败的反馈信息。车辆将随机数作为预设的对称加密算法的加密密钥对反馈信息进行了加密处理；将随机数作为对称加密算法的解密密钥对反馈信息进行解密处理，获得明文的反馈信息。

[0082] 具体的，反馈信息为字符串，用于提示终端车辆可以接收到数据但操作指令无法正常执行。在一个实施例中，反馈信息还包括执行失败的原因信息，以便于终端的用户及时做出调整。终端将获得明文的反馈信息以窗口的形式展示出来。

[0083] 在一个实施例中，如图4所示，提供的一种基于车载特种装备系统的数据加密传输系统，该系统包括车辆10和终端20。其中，

[0084] 终端20用于从服务器30下载公钥和车辆标识；接收用户对车辆标识对应的车辆触发的操作指令；生成随机数；通过公钥对包含随机数、操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据；通过无线网络将密文数据发送至车辆10；接收车辆10发送的执行结果；将随机数作为解密密钥对加密的执行结果进行解密，得到明文的执行结果；接

收车辆10发送的经过加密处理的反馈信息，将随机数作为预设的对称加密算法的解密密钥对反馈信息进行解密处理，获得明文的反馈信息。

[0085] 车辆10用于接收终端20发送的密文数据；通过私钥对密文数据进行解密处理获得随机数、操作指令以及用户信息的明文数据；校验用户信息是否合法并生成校验结果；当校验结果为是时，执行操作指令得到执行结果；将随机数作为对称加密算法的密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端20；当校验结果为否时，生成执行操作指令失败的反馈信息；将随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端20。

[0086] 本实施例中，终端、车辆以及服务器三者通过互联网建立连接。终端获得服务器授权后即可下载车辆标识和公钥。下载了公钥的终端与车辆之间可以通过数据加解密安全的传输数据。终端发送至车辆的操作指令包括但不限于：用户操控车辆的指令，例如，关闭车辆车门的指令。还可以是获取车辆状态数据的指令，例如，获取车辆油耗数据的指令。车辆执行操作指令返回至终端的数据包括但不限于：车辆的油耗数据、里程数据以及门或窗的开启状态数据，车辆的视频监控数据和拍照数据等。如图5所示，在一个实施例中，提供一种车载特种装备系统，该车载特种装备系统50包括：车载电脑501、无线收发器502、加解密器503以及校验器504；无线收发器502与加解密器503连接，加解密器503与校验器504连接，所述车载电脑501分别与所述加解密器503以及校验器504连接。

[0087] 加解密器503，用于存储车辆标识，生成包含公钥和私钥的密钥对，存储私钥，对终端发送的密文数据通过私钥进行解密处理，获得明文的随机数、操作指令以及用户信息；将随机数作为对称加密算法的密钥对执行结果和反馈信息进行加密处理。

[0088] 无线收发器502，用于接收终端发送的通过公钥对包含随机数、操作指令以及用户信息进行加密处理得到的密文数据，将加解密器对执行结果进行加密处理后的执行结果发送至终端。具体的，无线收发器包括GSM、GPRS、3G、4G、LTE、WIFI以及蓝牙中至少一种无线收发器。

[0089] 校验器504，用于获取加解密器传输的用户信息；校验用户信息是否合法，生成校验结果并传输至车载特种装备系统。

[0090] 校验器从加解密器的安全存储区域获取预先存储的用户信息(终端ID和/或用户ID)，与明文数据中的用户信息进行比较。若一致，则校验通过，则输出车载特种装备系统执行操作指令后得到的执行结果。例如，执行结果包括执行操作成功的信息或者获取车辆的状态数据。若不一致，则校验失败，则输出执行操作指令失败的反馈信息。

[0091] 车载电脑501，用于当校验结果为是时，执行操作指令，并将执行结果发送至加解密器中进行加密处理，当校验结果为否时，生成执行命令失败的反馈信息并发送至加解密器。

[0092] 本实施例中，车载特种装备系统中包括ECU(Electronic Control Unit，车载电脑)、CAN总线(Controller Area Network，控制器局域网络)以及OBD(On-Board Diagnostic，车载诊断系统)等功能部件。其中车载电脑用于执行操作指令。

[0093] 在一个实施例中，提供了一种安装有上述车载特种装备系统的车辆。该车辆为普通家用汽车以及其它类型的车辆。例如，军用车、警车以及特种车辆等。以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能

的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0094] 以上实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

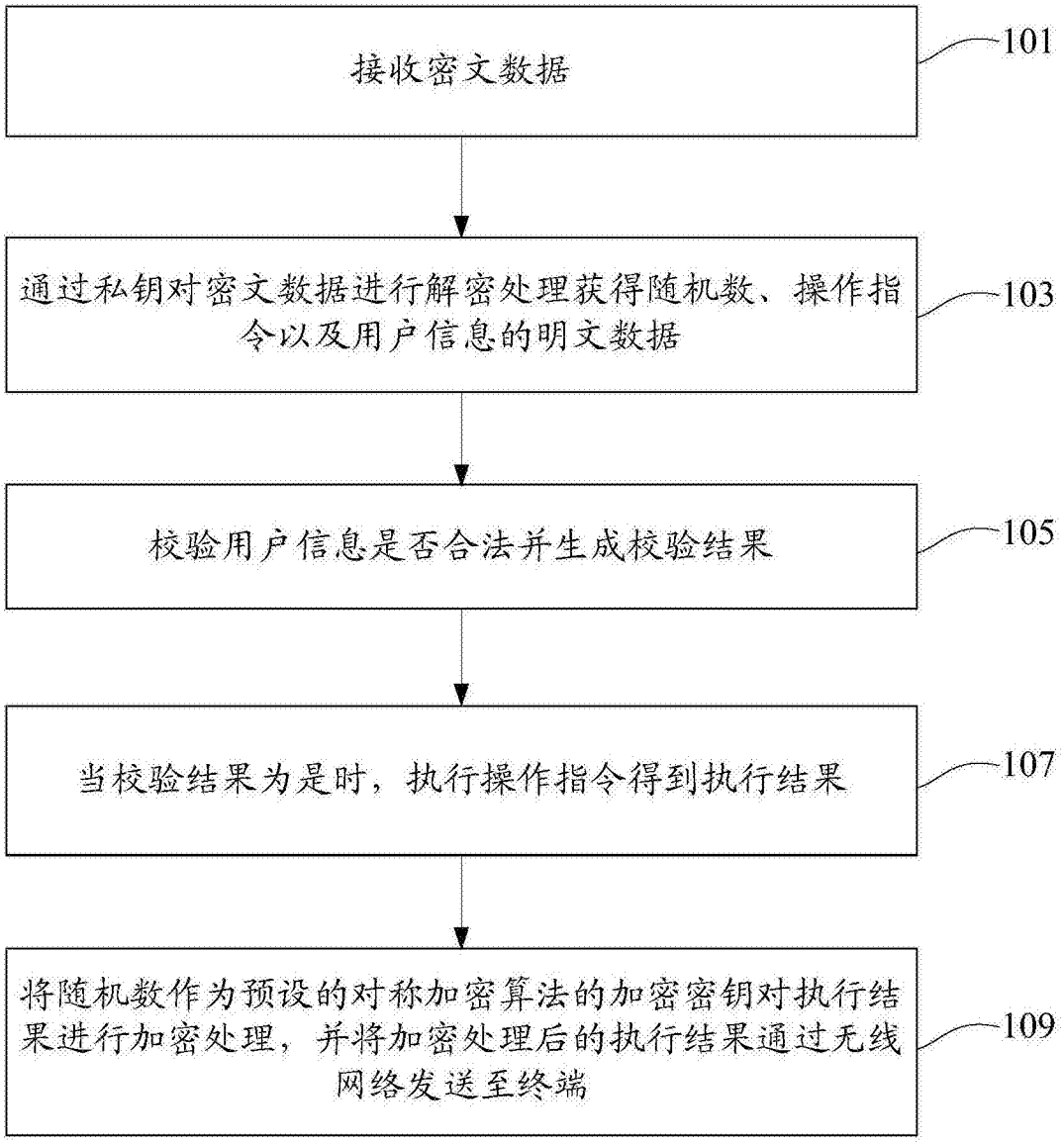

接收密文数据
101
通过私钥对密文数据进行解密处理获得随机数、操作指令以及用户信息的明文数据
103
校验用户信息是否合法并生成校验结果
105
当校验结果为是时，执行操作指令得到执行结果
107
将随机数作为预设的对称加密算法的加密密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端
109

图1

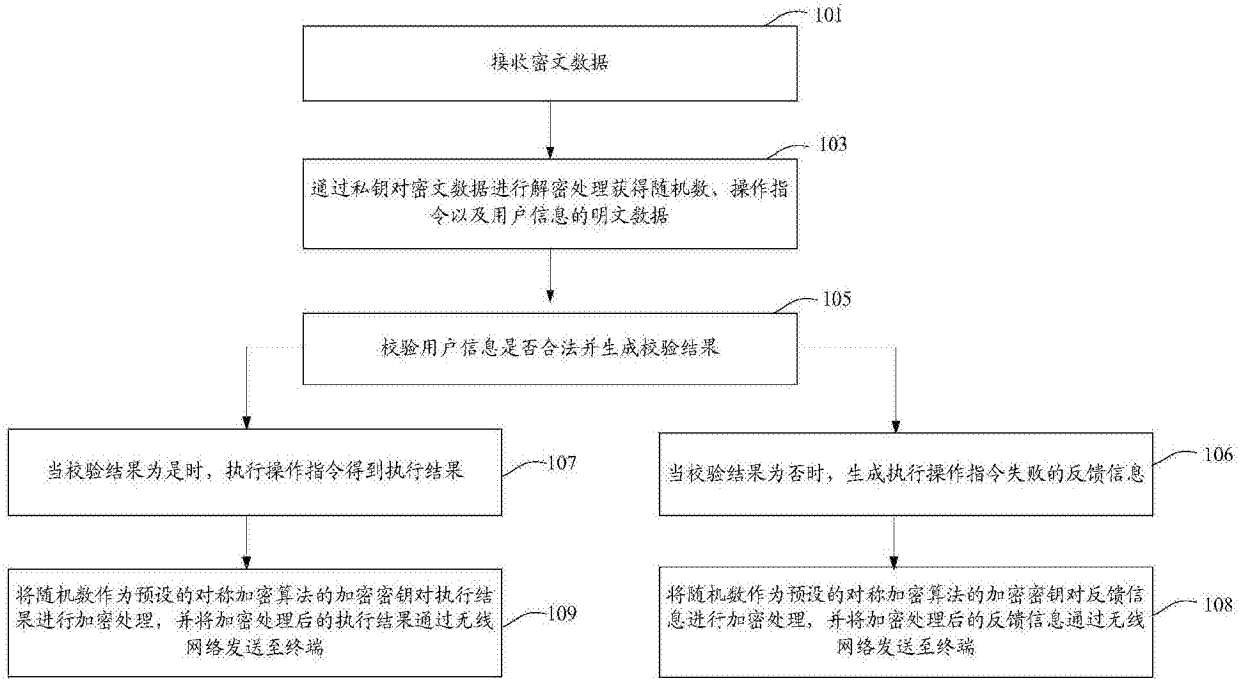

101
接收密文数据
103
通过私钥对密文数据进行解密处理获得随机数、操作指令以及用户信息的明文数据
105
校验用户信息是否合法并生成校验结果
当校验结果为是时，执行操作指令得到执行结果
107
将随机数作为预设的对称加密算法的加密密钥对执行结果进行加密处理，并将加密处理后的执行结果通过无线网络发送至终端
109
当校验结果为否时，生成执行操作指令失败的反馈信息
106
将随机数作为预设的对称加密算法的加密密钥对反馈信息进行加密处理，并将加密处理后的反馈信息通过无线网络发送至终端
108

图2

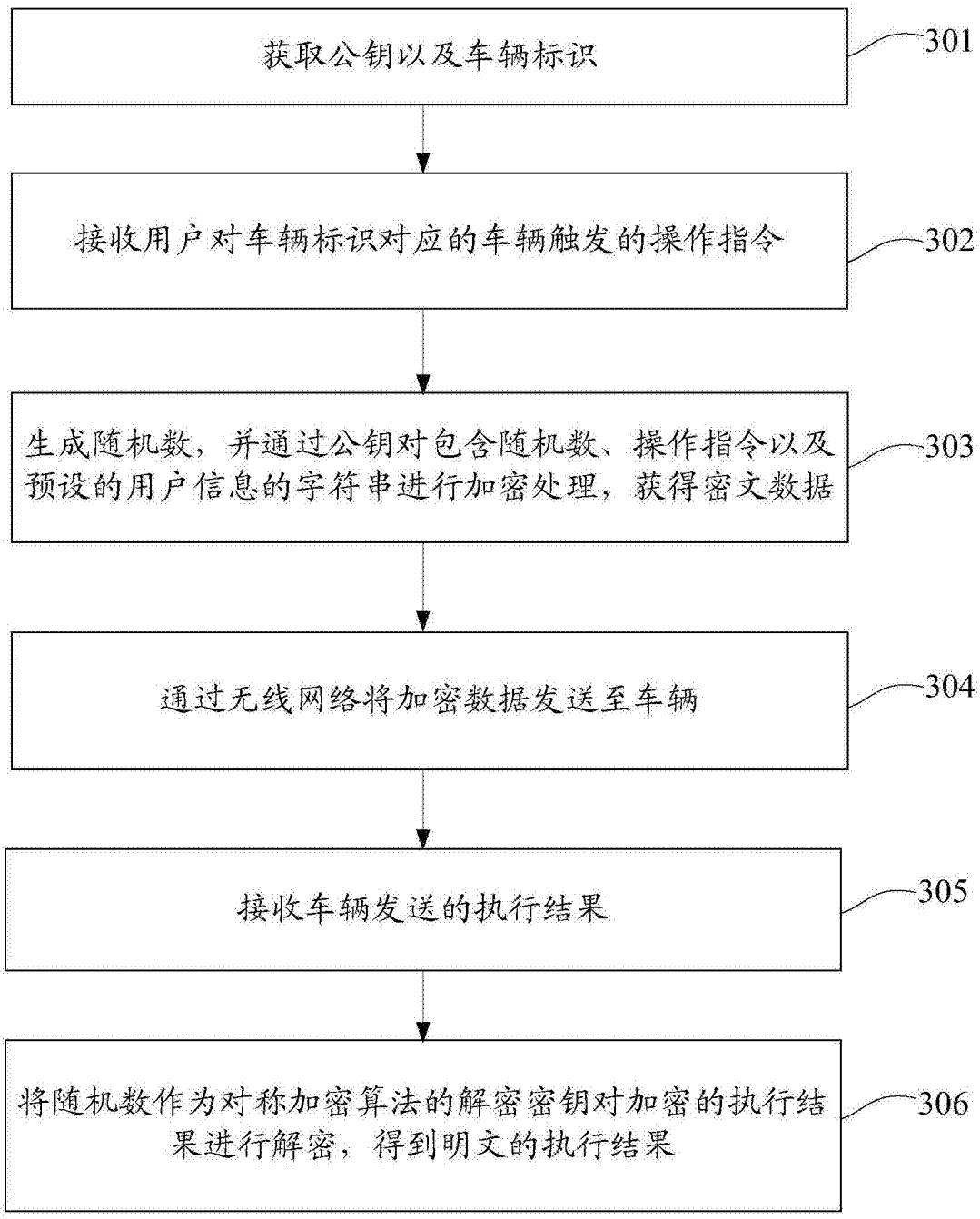

获取公钥以及车辆标识
301
接收用户对车辆标识对应的车辆触发的操作指令
302
生成随机数，并通过公钥对包含随机数、操作指令以及预设的用户信息的字符串进行加密处理，获得密文数据
303
通过无线网络将加密数据发送至车辆
304
接收车辆发送的执行结果
305
将随机数作为对称加密算法的解密密钥对加密的执行结果进行解密，得到明文的执行结果
306

图3

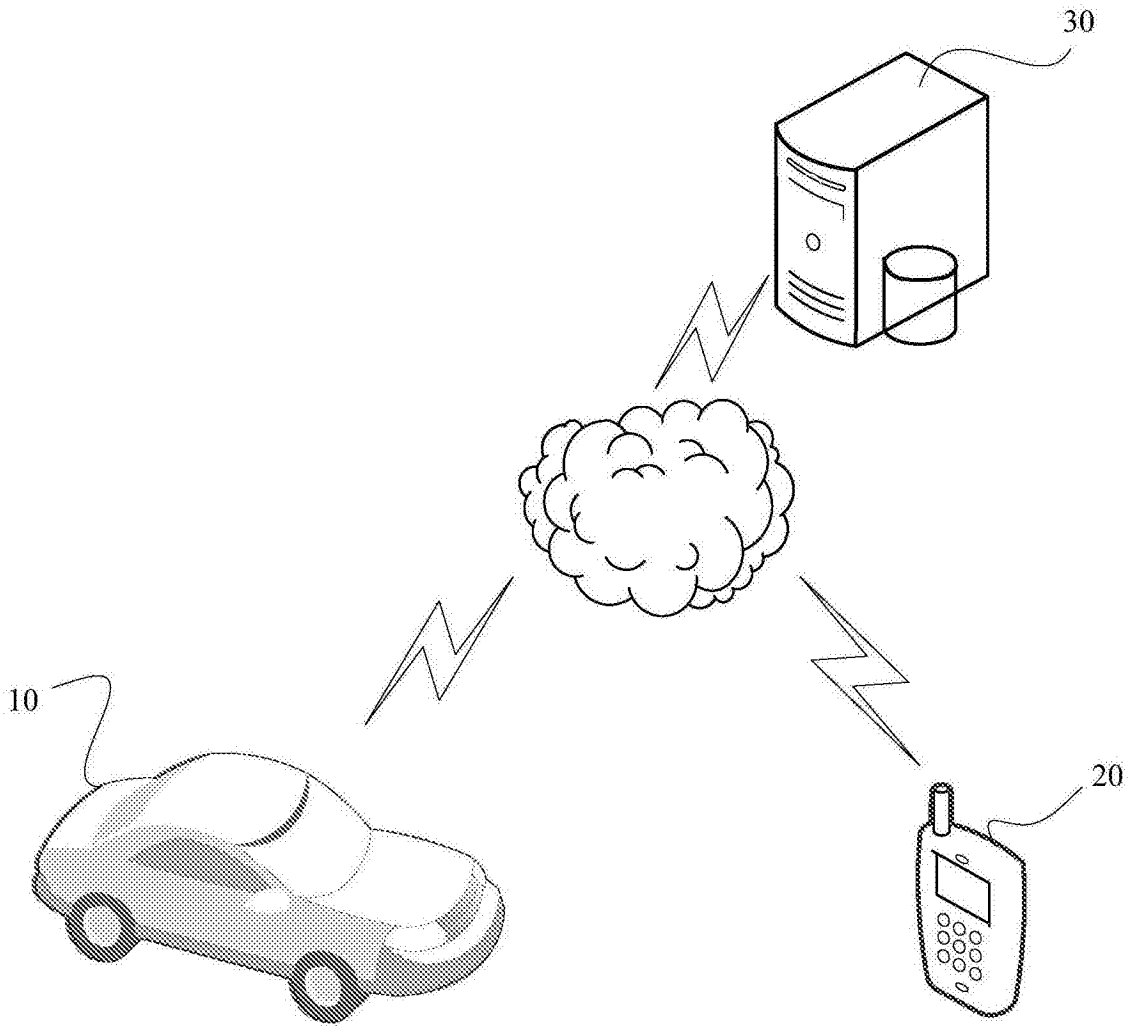


图4

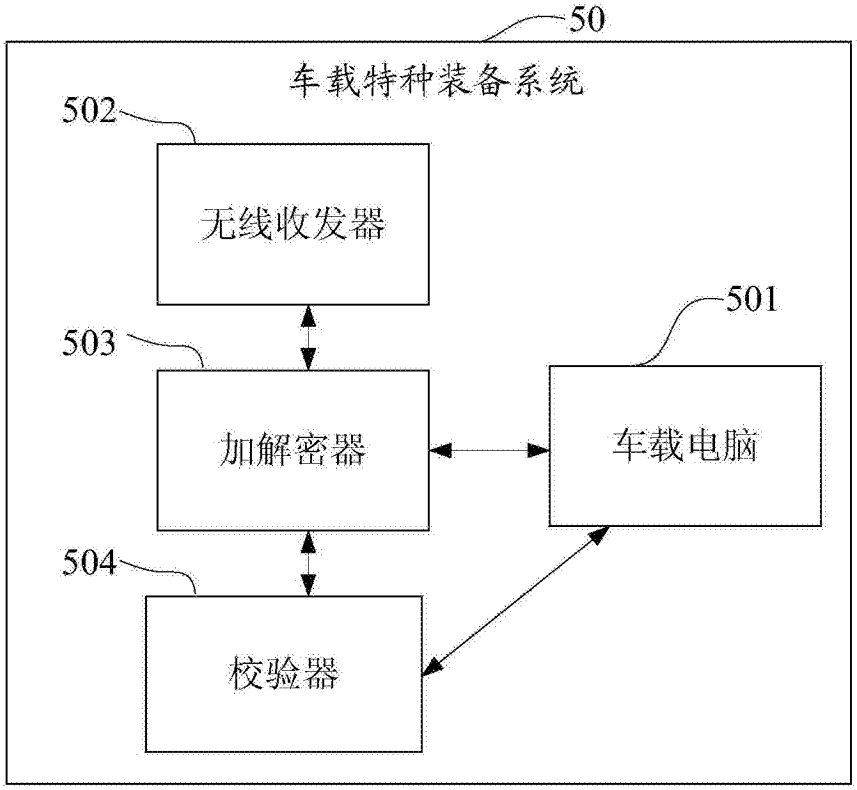


图5